CLAIMS

1. A method for implementing a network security level via a security switch, said security switch storing a modifiable list of trusted file extensions, said method as implemented in said network switch comprising the steps of:

(a) receiving a request from a client to a server;

(b) parsing and identifying a file extension associated with said received request;

(c) comparing said identified file extension with said pre-stored list of trusted file extensions; and

(d) forwarding the received request to an inspection gateway a upon not finding a successful match.

2. A method as per claim 1, wherein upon finding a successful match in step (c) forwarding said received request to said server.

3. A method as per claim 1, wherein said steps (a) through (d) are performed upon verifying that said client is an authorized client.

4. A method as per claim 1, wherein said steps (a) through (d) are performed upon verifying that said server is an authorized server.

5. A method as per claim 1, wherein said security switch stores a modifiable list of trusted content-types, said method further comprising the steps of:

receiving a reply from said server;

parsing said reply to identify a content-type of an object contained in said reply;

comparing said identified content-type with said pre-stored list of trusted content-types; and

upon finding a successful match, forwarding said reply to said client.

6. A method as per claim 1, wherein said request is a HTTP request.

7. A method as per claim 1, wherein communication session between said client and said server is a TCP/IP session.

8. A method as per claim 1, wherein said object is any of the following: an image file, an audio file, a video file, an active server page file, a script file, or a markup language-based file.

9. A method as per claim 1, wherein said security switch communicates with said server over a network, and said network is any of the following: local area network (LAN), wide area

network (WAN), metropolitan area network (MAN), wireless network, cellular network, or the Internet.

10. An article of manufacture comprising a computer usable medium having computer readable program code embodied therein implementing a network security level via a modifiable list of trusted file extensions, said medium comprising:

(a) computer readable program code aiding in receiving a request from a client to a server;

(b) computer readable program code parsing and identifying a file extension associated with a received request;

(c) computer readable program code comparing an identified file extension with said pre-stored list of trusted file extensions; and

(d) computer readable program code aiding in forwarding the received request to an inspection gateway.

11. A method as per claim 10, wherein the computer readable program code causes the forwarding of the received request to an inspection gateway upon not finding a successful match, and wherein upon finding a successful match, further comprising:

(1) computer readable program code forwarding a received request to a server;

(2) computer readable program code receiving a reply from a server; and

(3) computer readable program code aiding in forwarding a reply to a client.

12. An article of manufacture as per claim 10, wherein said medium further comprises:

computer readable program code parsing a reply to identify a content-type of an object contained in said reply;

computer readable program code comparing an identified content-type with a pre-stored list of trusted content-types; and

upon finding a successful match, computer readable program code forwarding said reply to said client.

13. A method for implementing a network security level via a security switch, said security switch storing a modifiable list of trusted file extensions and a modifiable list of trusted content-types, said method as implemented in said network switch comprising the steps of:

(a) receiving a request from a client to a server;

(b) parsing and identifying a file extension associated with said received request;

(c) comparing said identified file extension with said pre-stored list of trusted file extensions; and

(d) forwarding said received request to an inspection gateway upon not finding a successful match.

14. A method as per claim 13, wherein upon finding a successful match, further comprising:

(1) forwarding said received request to said server;

(2) receiving a reply from said server,

(3) parsing said reply to identify a content-type of an object contained in said reply;

(4) comparing said identified content-type with said pre-stored list of trusted content-types; and

(5) upon finding a successful match, forwarding said reply to said client.

15. A method as per claim 13, wherein said steps (a) through (d) are performed upon verifying that said client is an authorized client.

16. A method as per claim 13, wherein said steps (a) through (d) are performed upon verifying that said server is an authorized server.

17. A method as per claim 13, wherein said request is a HTTP request and a communication session between said client and said server is a TCP/IP session.

18. A method as per claim 13, wherein said object is any of the following: an image file, an audio file, a video file, an active server page file, a script file, or a markup language-based file.

19. A method as per claim 13, wherein said security switch communicates with said server over a network, and said network is any of the following: local area network (LAN), wide area network (WAN), metropolitan area network (MAN), wireless network, cellular network, or the Internet.

20. A system implementing network security for content exchanged between a client and a server over a network, said system comprising:

(a) a security switch storing a modifiable list of trusted file extensions, said security switch:

receives and parses requests to identify a file extension associated with a received request;

compares said identified file extension with said pre-stored list of trusted file extensions; and

upon finding a successful match, forwards said received request to said server and receives a reply from said server; and

(b) an inspection gateway working in conjunction with said security switch and receiving forwarded requests when a file extension of a request fails to match trusted file

extensions in said pre-stored list, said inspection gateway communicating with said server and retrieving, inspecting, and verifying an object related to said received request, and based upon successful verification, forwarding a reply to said security switch.

21. A system as per claim 20, wherein said security switch further comprises a modifiable list of trusted content-types, and said security switch after reception of said reply from said server,

parses said reply to identify a content-type of an object contained in said reply;

compares said identified content-type with said pre-stored list of trusted content-types; and

upon finding a successful match, forwards said reply to said client.

22. A system as per claim 20, wherein said request is an HTTP request and communication between said client and server is via a TCP/IP session.

23. A system as per claim 20, wherein said object is any of the following: an image file, an audio file, a video file, an active server page file, a script file, or a markup language-based file.

24. A system as per claim 20, wherein said security switch communicates with said server over a network, and said network is any of the following: local area network (LAN), wide

area network (WAN), metropolitan area network (MAN), wireless network, cellular network, or the Internet.

25. An article of manufacture comprising a computer usable medium having computer readable program code embodied therein implementing a network security level via a modifiable list of trusted file extensions and a modifiable list of trusted content-types, said medium comprising:

(a) computer readable program code aiding in receiving a request from a client to a server;

(b) computer readable program code parsing and identifying a file extension associated with a received request;

(c) computer readable program code comparing an identified file extension with said pre-stored list of trusted file extensions; and

(d) computer readable program code aiding in forwarding said received request to an inspection gateway upon finding a successful match,

26. The medium of claim 25 further comprising:

(1) computer readable program code aiding in forwarding a received request to a server;

(2) computer readable program code aiding receiving a reply from a server;

(3) computer readable program code parsing a reply to identify a content-type of an object contained in said reply;

(4) computer readable program code comparing an identified content-type with said pre-stored list of trusted content-types; and

(5) computer readable program code aiding in forwarding a reply to a client upon finding a successful match.

27. The medium as per claim 26, wherein when said computer readable program code compares an identified file extension with said pre-stored list of trusted file extensions and does not find a match said computer readable program code of (1) through (5) is executed.

28. A method for implementing a network security level via a security switch, said method as implemented in said network switch comprising the steps of:

(a) receiving a request from a client to a server;

(b) parsing and identifying a file extension associated with said received request;

(c) verifying said identified file extension as a trusted file extension; and

(d) upon not verifying said identified file extension, forwarding the received request to an inspection gateway; else forwarding said received request to said server.

29. A method as per claim 28, said method further comprising the steps of:

receiving a reply from said server;

parsing said reply to identify a content-type of an object contained in said reply;

verifying said identified content-type as a trusted content-type; and

upon verifying said identified content-type, forwarding said reply to said client.

30. A method as per claim 28, wherein said steps (a) through (d) are performed upon verifying that said client is an authorized client.

31. A method as per claim 28, wherein said steps (a) through (d) are performed upon verifying that said server is an authorized server.

32. A method for implementing a network security level via a security switch, said method as implemented in said network switch comprising the steps of:

(a) receiving a request from a client to a server;

(b) verifying said received request as a trusted request; and

(c) upon not verifying said received request, forwarding said received request to an inspection gateway; else forwarding said received request to said server.

33. A method as per claim 32, said method further comprising the steps of:

receiving a reply from said server;

parsing said reply to identify a type of an object contained in said reply;

verifying said identified type of object as a trusted object type; and

upon verifying said identified type of object, forwarding said reply to said client, else, not forwarding said reply to said client.

34. A method as per claim 32, wherein said steps (a) through (c) are performed upon verifying that said client is an authorized client.

35. A method as per claim 32, wherein said steps (a) through (c) are performed upon verifying that said server is an authorized server.